PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-005785
(43)Date of publication of application : 12.01.2001

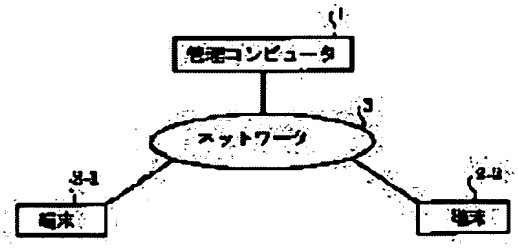
(51)Int.CI. G06F 15/00
H04L 9/32

(21)Application number : 11-176276
(22)Date of filing : 23.06.1999

(71)Applicant : MATSUMOTO MAKOTO
(72)Inventor : MATSUMOTO MAKOTO

(54) DIGITAL AUTHENTICATING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent key leakage to the third person in a one-time password system.
SOLUTION: A host computer 1 transmits random number data to client terminals 2-1 and 2-2. The terminals 2-1 and 2-2 receive the random number data from the computer 1, and the random number data are shown on the displays of the terminals 2-1 and 2-2. A client overlaps a storage key on this display and inputs a password according to an input order designated by the storage key. The password is transmitted to the computer 1. The computer 1 retrieves the received data string by using the same storage key, and when it coincides with the received data string, the computer 1 decides the data string as the password of the client and authenticates the client.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－5785
（Ｐ2001－5785Ａ）
(43)公開日　平成13年1月12日(2001.1.12)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ06Ｆ 15/00	330	Ｇ06Ｆ 15/00	330Ｅ	5Ｂ085
Ｈ04Ｌ 9/32		Ｈ04Ｌ 9/00	673Ａ	5Ｊ104
			675Ａ	

審査請求　未請求　請求項の数6　ＯＬ　（全９頁）

(21)出願番号　特願平11－176276

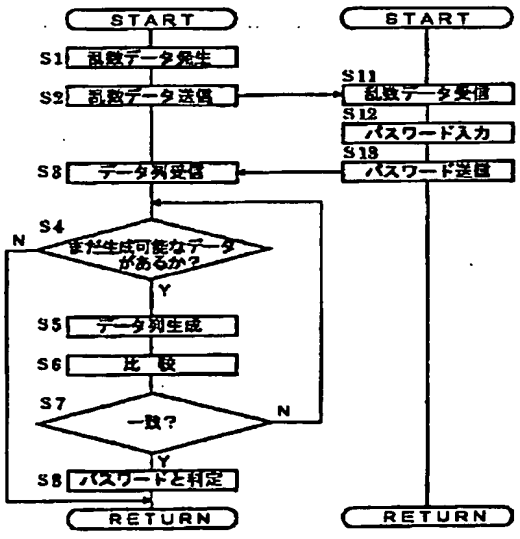
(22)出願日　平成11年6月23日(1999.6.23)

(71)出願人　599087464
松本　眞
福岡県福岡市東区箱崎１－13－10　八千代ビル302
(72)発明者　松本　眞
福岡県福岡市東区箱崎１－13－10　八千代ビル302
(74)代理人　100082050
弁理士　佐藤　幸男　（外１名）

Ｆターム(参考)　5Ｂ085 ＡＥＤ3 ＡＥＤ8 ＡＥ15
5Ｊ104 ＡＡ07 ＡＡ16 ＥＡ03 ＫＡ01 ＫＡ04 ＮＡ02 ＮＡ03 ＮＡ05 ＰＡ07

(54)【発明の名称】　電子認証装置

(57)【要約】
【課題】　ワンタイムパスワードシステムでのキーの第三者への漏洩を防止する。
【解決手段】　ホストコンピュータ１は、乱数データを顧客の端末２－１，２－２に送信する（Ｓ２）。端末２－１，２－２は、ホストコンピュータ１から乱数データを受信し（Ｓ１１）、乱数データが端末２－１，２－２のディスプレイ上に表示される。顧客は記憶キーをこのディスプレイに重ね、記憶キーによって指定された入力順に従ってパスワードを入力する。このパスワードはホストコンピュータ１に送信される（Ｓ１３）。ホストコンピュータ１は、同じ記憶キーを用いて受信したデータ列を検索し、受信したデータ列と一致したときは、このデータ列は顧客のパスワードと判定して顧客の認証を行う（Ｓ３～８）。



具体例１の動作を示すフローチャート

1

【特許請求の範囲】

【請求項1】 顧客を管理するホストコンピュータと複数の端末とが接続されたネットワーク上で、ホストコンピュータから顧客の端末に所定の乱数データを送信し、顧客の端末からホストコンピュータに、該乱数データの中から所定の入力順に従って入力されたパスワードを送信し、ホストコンピュータが、受信したパスワードの真偽を判定して顧客の認証を行う電子認証装置において、

前記ホストコンピュータは、顧客からアクセス要求を受けたとき、顧客の端末に、乱数データを送信する乱数データ送信手段と、

該乱数データの送信に呼応して返信されたデータ列を受信するデータ列受信手段と、

前記乱数データをディスプレイ上に2次元に配列し、選択する文字の入力順序を指定する所定形状の暗号鍵を、ディスプレイ上に重ね合わせることによって選択可能な複数のデータ列を生成するデータ列生成手段と、

該データ列生成手段によって生成された複数のデータ列の中に、受信したデータ列と一致するものがあるときは、受信したデータ列は顧客の端末から送信されたパスワードと判定し、顧客の認証を行う認証手段と、を備え、

各端末は、ホストコンピュータから送信された乱数データを受信する乱数データ受信手段と、

受信した乱数データをディスプレイ上に2次元に配列し、ホストコンピュータで用いたものと同じ暗号鍵をディスプレイ上に重ねて選択された複数の文字に基づいて生成されたパスワードを、ホストコンピュータに送信するパスワード送信手段と、を備えたことを特徴とする電子認証装置。

【請求項2】 前記ホストコンピュータの乱数データ送信手段は、異なる形状の文字データを混在させて乱数データを送信するように構成されたことを特徴とする請求項1に記載の電子認証装置。

【請求項3】 前記端末のパスワード送信手段は、生成されたパスワードに対して所定の第1の演算を行い、当該演算結果に対して桁落としをして送信するように構成され、

前記ホストコンピュータのデータ列生成手段は、データ列生成手段によって生成されたデータ列に対して端末のパスワード送信手段と同じ第1の演算及び桁落としを行って所定のデータ列を生成するように構成されたことを特徴とする請求項1又は請求項2に記載の電子認証装置。

【請求項4】 前記端末のパスワード送信手段及びホストコンピュータのデータ列生成手段が行う第1の演算は、生成されたパスワードに基づいて複数のデータを生成し、当該複数のデータを用いて複数のデータに依存するデータを算出する第2の演算と、該第2の演算によって演算された演算結果の各桁の数値に依存するデータを

2

算出する第3の演算と、を含んだ演算であることを特徴とする請求項3に記載の電子認証装置。

【請求項5】 前記第2の演算は複数のデータに対して行う所定の二項演算であって、第3の演算は、第2の演算によって演算された演算結果に対して行う演算であって1つの数値から1つの数値を得る単項演算であることを特徴とする請求項4に記載の電子認証装置。

【請求項6】 前記ホストコンピュータは、認証手段により顧客の認証が行われたとき、当該顧客の端末に、桁落としによって送信されなかった文字を返信するように構成されたことを特徴とする請求項4又は請求項5に記載の電子認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子認証装置に関する。

【0002】

【従来の技術】近年、例えば、銀行のような管理者と銀行の顧客との間で自動取り引き機を用いて行う取引が増えてきている。

【0003】また、複数の顧客がある管理者に対して顧客登録し、自宅又は移動先のパーソナルコンピュータと管理者用のホストコンピュータとを電話回線等でネットワーク接続し、顧客がパーソナルコンピュータから電話回線等を介して電子的な方法でホストコンピュータに接続して取引を行う動きも多くなってきている。

【0004】このような取引において、顧客がホストコンピュータにアクセスしたときに、ホストコンピュータ側で、登録した顧客本人であるかどうかを認証する必要がある。

【0005】この認証を行う場合、以下のような可能性が考えられる。

（1）第三者に通信が傍受される可能性

（2）顧客が使う端末（コンピュータ）が顧客専用のものでないとき、顧客が端末に入力したデータが端末に保存され、このデータが第三者に漏洩するという可能性

（3）顧客の端末に罠がしかけられ、顧客のパスワードが盗まれる可能性

【0006】従って、安全な取引を行うためには、このような可能性を排除しなければならない。このような可能性を排除した電子認証装置として、ワンタイムパスワード（one time password）を用いたものがある。

【0007】図9は、ワンタイムパスワードを用いた電子認証装置の動作を示す説明図である。顧客を管理するホストコンピュータにアクセスするときは、顧客端末からホストコンピュータに顧客IDを送信し、ホストコンピュータは顧客IDを受信して乱数データ「17628 49579」を顧客の端末に送信する。顧客とホストコンピュータの管理者は例えば暗証番号のような同じ記憶キー「8523」を予め所持しておく。

【0008】この記憶キー「8523」の数値は桁数を示す。この記憶キー「8523」を用いて乱数データ「1762849579」の8，5，2，3桁目の数値「5」，「8」，「7」，「6」が取り出される。このデータ「5876」がワンタイムパスワードとなり、このワンタイムパスワードがホストコンピュータに送信される。

【0009】乱数データの送信主であるホストコンピュータは、ワンタイムパスワード「5876」を受信して顧客が用いたのと同じ記憶キー「8523」を用い、乱数データ「1762849579」からデータ列「5876」を生成する。このデータ列「5876」は受信したワンタイムパスワードと一致するので、このパスワードは顧客から送られたものと判定して顧客を認証する。このようなワンタイムパスワードを用いることにより、上記（1）～（3）の危険が防止される。

【0010】

【発明が解決しようとする課題】しかしながら、かかる従来の電子認証装置では、通信回線上で乱数データ及びワンタイムパスワードが何度も傍受された場合、あるいは乱数データが顧客端末に残存してワンタイムパスワードが漏洩した場合には、数値の組み合わせが少ないため、記憶キーは簡単に見破られてしまう。

【0011】例えば、図において、乱数データ「1762849579」及びワンタイムパスワード「5876」に基づいて考えられる桁は、第8，5，2，3桁又は第8，5，9，3桁だけである。従って、顧客が再度ワンタイムパスワードを送信すれば顧客の記憶キーは「8523」であることが見破られてしまう。

【0012】このようなパスワードは、特に、選択できるデータ数（10進数のときは10、アルファベット文字のときは26）に比べて乱数データの桁数がそれほど大きくない場合に漏洩するおそれが大きい。従って、ワンタイムパスワードでの、キーの第三者への漏洩を防止する必要がある。

【0013】

【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

〈構成1〉請求項1の発明に係る電子認証装置では、前記ホストコンピュータが、顧客からアクセス要求を受けたとき、顧客の端末に、乱数データを送信する乱数データ送信手段と、該乱数データの送信に呼応して返信されたデータ列を受信するデータ列受信手段と、前記乱数データをディスプレイ上に2次元に配列し、選択する文字の入力順序を指定する所定形状の暗号鍵を、ディスプレイ上に重ね合わせることによって選択可能な複数のデータ列を生成するデータ列生成手段と、該データ列生成手段によって生成された複数のデータ列の中に、受信したデータ列と一致するものがあるときは、受信したデータ列は顧客の端末から送信されたパスワードと判定し、顧客の認証を行う認証手段と、を備え、各端末が、ホストコンピュータから送信された乱数データを受信する乱数データ受信手段と、受信した乱数データをディスプレイ上に2次元に配列し、ホストコンピュータで用いたものと同じ暗号鍵をディスプレイ上に重ねて選択された複数の文字に基づいて生成されたパスワードを、ホストコンピュータに送信するパスワード送信手段と、を備えて構成されている。

【0014】〈構成2〉請求項2の発明に係る電子認証装置では、前記ホストコンピュータの乱数データ送信手段が、異なる形状の文字データを混在させて乱数データを送信するように構成されている。

【0015】〈構成3〉請求項3の発明に係る電子認証装置では、前記端末のパスワード送信手段が、生成されたパスワードに対して所定の第1の演算を行い、当該演算結果に対して桁落としをして送信するように構成され、前記ホストコンピュータのデータ列生成手段は、データ列生成手段によって生成されたデータ列に対して端末のパスワード送信手段と同じ第1の演算及び桁落としを行って所定のデータ列を生成するように構成されている。

【0016】〈構成4〉請求項4の発明に係る電子認証装置では、前記端末のパスワード送信手段及びホストコンピュータのデータ列生成手段が行う第1の演算が、生成されたパスワードに基づいて複数のデータを生成し、当該複数のデータを用いて複数のデータに依存するデータを算出する第2の演算と、該第2の演算によって演算された演算結果の各桁の数値に依存するデータを算出する第3の演算と、を含んだ演算である。

【0017】〈構成5〉請求項5の発明に係る電子認証装置では、前記第2の演算が複数のデータに対して行う所定の二項演算であって、第3の演算は、第2の演算によって演算された演算結果に対して行う演算であって1つの数値から1つの数値を得る単項演算である。

【0018】〈構成6〉請求項6の発明に係る電子認証装置では、前記ホストコンピュータが、認証手段により顧客の認証が行われたとき、当該顧客の端末に、桁落としによって送信されなかった文字を返信するように構成されている。

【0019】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。

〈具体例1〉具体例1は、乱数データの中から顧客が所定形状の記憶キーを用いて複数の文字を選択してパスワードを生成し、ホストコンピュータ側でも同じ記憶キーを用いて受信したパスワードに基づいて顧客の認証を行うようにしたものである。

【0020】図1は、具体例1の構成を示すブロック図である。ホストコンピュータ1は、顧客を管理すると共に、乱数データを送信し、受信したデータ列に基づいて

顧客の認証を行うためのコンピュータである。

【００２１】端末２－１，２－２は、ホストコンピュータ１から乱数データを受信し、顧客が入力したパスワードを送信するための端末である。このホストコンピュータ１及び端末２－１，２－２は、ネットワーク３を介して接続されている。

【００２２】図２は、ホストコンピュータ１、端末２－１，２－２の構成を示すブロック図である。この図２に示すように、ホストコンピュータ１及び端末２－１，２－２は、それぞれＣＰＵ１１と、ＲＯＭ１２と、ＲＡＭ１３と、記憶装置１４を備えて構成されている。このホストコンピュータ１の記憶装置１４には、顧客のＩＤ、暗号鍵としての記憶キー等が格納されている。

【００２３】〈動作〉次に具体例１の動作を説明する。図３は具体例１の動作を示すフローチャートである。尚、ステップ（図中、ステップを「Ｓ」と記す。）１～７はホストコンピュータ１が実行するステップであり、ステップ１１～１３は顧客の端末２－１，２－２が実行するステップである。

【００２４】ホストコンピュータ１は顧客の端末２－１，２－２から顧客ＩＤを受信したとき、ステップ１を実行し、乱数データを生成する。乱数データは、アルファベット、あるいは数値によって構成されている。

【００２５】ステップ２では、この乱数データをアクセスを要求した顧客の端末２－１，２－２に送信する。顧客の端末２－１，２－２はステップ１１の実行により、ホストコンピュータ１から乱数データを受信する。

【００２６】この乱数データはアルファベットのランダムパターンとして端末２－１，２－２のディスプレイ上に２次元に配列される。図４は２次元に配列されたランダムパターンの一例を示す説明図である。

【００２７】ステップ１２では、顧客が入力した複数の文字に基づいてパスワードを生成する。図５は顧客が用いる記憶キーの一例を示す説明図である。番号１～１６はランダムパターン上でパスワードの文字の入力順を指定する番号である。この記憶キーは管理者から顧客に送付される。尚、記憶キーをホストコンピュータ１からネットワーク３を介して顧客の端末２－１，２－２に予め送信してもよいし、郵送してもよい。

【００２８】顧客はランダムパターンに対して記憶キーを適当に平行移動させ、任意の位置でランダムパターン上に重ね合わせ、記憶キーの番号１～１６に従って順番にデータを入力する。例えば、図５に示す記憶キーを図４に示すランダムパターンの左上端に配置したとき、記憶キーの番号１～１６に従って順番にデータを入力すれば、「APDGFXEKN2QFSAWB」というデータ列が得られる。このデータ列「APDGFXEKN2QFSAWB」がワンタイムパスワードとなる。

【００２９】ステップ１３では、作成したパスワードを送信する。次に、ホストコンピュータ１はステップ３を実行し、データ列を受信してステップ４に進む。

【００３０】ステップ４では、ランダムパターン及び記憶キーを用いて生成できるデータ列があるかどうかを判定する。データ列を生成できるときはステップ５に進む。

【００３１】ステップ５では、図４に示すように、顧客に送ったものと同じ乱数データをディスプレイ上に２次元に配列する。そして、図５に示すような顧客と同じ記憶キーをこのディスプレイの所定の位置に重ね合わせ、この記憶キーによって指定された順序で文字を選択し、データ列を生成する。

【００３２】ステップ６では、生成したデータ列をステップ３において受信したデータ列と比較する。ステップ７では、この両データ列が一致するかどうかを判定する。例えば、顧客からワンタイムパスワードを受信し、顧客と同じ記憶キーを用いて、顧客と同じランダムパターン上でこの記憶キーを移動させれば、受信したデータ列と一致するデータ列が得られるはずである。

【００３３】例えば、図４、５に示すような顧客と同じランダムパターン及び記憶キーを用い、記憶キーをディスプレイ上で移動させてデータ列を生成すれば、このデータ列のうちのいずれか１つに該当するデータ列を受信するはずである。このときは、ステップ８に進み、受信したデータ列は顧客のワンタイムパスワードであると判定する。

【００３４】また、両データ列が不一致のときは、ステップ４に戻り、ステップ４～７を実行する。傍受を試みる第三者からデータ列を受信したときは、顧客と同じランダムパターン及び記憶キーを用いてデータ列を生成しても、この生成されたＮ通りのデータ列の中に、受信したデータ列と一致するものは現れない。このときは、ステップ４において、受信したデータ列は顧客のパスワードではないと判定してこのルーチンを終了する。

【００３５】このような方式では、第三者が記憶キーを推測するのは非常に困難となる。例えば、入力されたパスワードの列を$x1, x2, \cdots, xk$、ランダムな二次元アルファベットテーブルの列を$T1, T2, \cdots, Tk$として情報がｋ回漏洩した場合に、バックトラック探索を行って記憶キーの内容を推測する方法を考える。

【００３６】まず、ランダムパターンに使う文字の集合の大きさＤを考える。ランダムパターンにアルファベットの文字（ａ～ｚ）を使った場合は、Ｄ＝２６であり、数字（０～９）を使った場合は、Ｄ＝１０である。また、ランダムパターンに含まれる升目の数をＮとする。図４の例では、Ｎ＝３０×３０＝９００である。

【００３７】まず、顧客の記憶キーＰの大きさを推測し、記憶キーがすっぽり入る大きさの長方形Ｒを作る。この長方形の中の升目の数をＳとする。図５の例では、Ｓ＝７×７＝４９である。記憶キーＰの一部分を推測する。パターンＰの最初のｍ個までがなす部分パターンを

Ｐｍとする。例えば、部分パターンＰ９は最初の９個までがなすパターンである。

【００３８】前記長方形Ｒに含まれるすべての順序付きｍ桁からなる集合Ｘを考える。したがって、集合Ｘは、Ｓ＾ｍ個の元からなる。Ｐｍは、このうちの１つであり、第三者はそれがどれであるかを推測する。

【００３９】集合Ｘの元をランダムにとり、Ｑとする。第三者はＱがＰｍであるかどうかを調べる。そのために、第三者は、二次元アルファベットテーブルＴ１に対し、Ｑをどこかに置けば列ｘ１の最初のｍ桁を生成しうるかどうかを全数検索する。どこにおいてもｘ１の最初のｍ桁を生成しなければ、ＱはＰｍではない。よって、ＱはＰｍの候補から棄却される。

【００４０】Ｑの位置を一つ決めたとき、Ｑがｘ１の最初のｍ桁を生成する確率は、

１／（Ｄ＾ｍ）

である。第三者が、たとえトラップをしかけようとも、Ｑをおいた位置という情報はもれない（画面上に記憶キーを置く位置は、端末コンピュータにわからないから）。

【００４１】テーブルが大きければ、Ｑを置きうる場所はおよそＮ個であるから、Ｎ個全部を調べたときどれもがｘ１を生成しない確率は、

p1=(1-1/(D^m))^N

であり、近似的に

p1=1-N/(D^m)

このとき、ＱはＴ１，ｘ１に適合しないので棄却される。

【００４２】これをｋ個のテーブルＴ１，・・・，Ｔｋ、データｘ１，・・・，ｘｋについて行えば、全てのテストで棄却されない確率は、

p2=(1-p1)^k

である。近似的には、

p2=N^kd^(-km)

である。この確率ｐ２で、Ｑはｋ回のテスト全てに合格する。

【００４３】Ｐｍは上記ｋ回のテスト全てに合格する。第三者は、Ｘの全ての元Ｑに対し、このテストを行い、合格したＱをもってＰｍと推測する。Ｘの元のうち合格する元の数の期待値をＣとすると、近似的に

C=S^m×p2=S^m/((D^m/N)^k)

となる。Ｃが大きければ第三者には推測が困難である。

【００４４】Ｃ＝１，即ち、Ｐｍが一意に確定してしまうのに要する漏洩の回数ｋは、

k=(m×logS)/(log(D^m/N))=(m×logS)/((m×logD)-logN)

となる。ｍが増えるに従って上記ｋは減少する、即ち、少ない回数の漏洩で記憶キーのｍ桁目までが漏洩するようになる。しかし、その場合Ｘの元の数Ｓ^ｍが増大し、全数チェックが困難となる。

【００４５】Ｓ＝64のとき、ｍ＝８程度で全数チェックは困難となる。Ｄ＝10,Ｎ＝1000,のときは、

K=8×８/(8×3.3-10)＝４（近似）

となり、情報の漏洩が４回未満であれば記憶キーを一意に特定することは困難である。

【００４６】また、ホストが受理するパスワードの総数は、一つのランダムパターンについてたかだかＮ個である。従って、まったくの偶然により第三者からのでたらめなパスワードにより認証が行われる確率ｐ３は、記憶キーの桁数をｗとしたとき、

p3=N/(D^w)

となる。例えば、図４，５ではＤ＝10、Ｎ＝900、ｗ＝１０なので、この確率は100万分の１以下となる。従って、偶然に認証が行われることはほとんどなく、顧客の認証を行うことができる。

【００４７】尚、ステップ２が乱数データ送信手段に、ステップ３がデータ列受信手段に、ステップ５がデータ列生成手段に、ステップ６～８が認証手段に、ステップ１１が乱数データ受信手段に、ステップ１３がパスワード送信手段に相当する。

【００４８】〈効果〉以上、説明したように具体例１によれば、ホストコンピュータ１から乱数データを送信し、顧客は記憶キーを用いてパスワードを入力するので、第三者によって記憶キー等の情報の漏洩を確実に防止することができる。

【００４９】また、乱数データがランダムパターンとしてディスプレイ上に表示されるので、たとえパスワードの文字数が多くても顧客は記憶キーを用いて分かりやすい状態でパスワードを入力することができる。さらに、ランダムパターン全体を使ってパスワードのデータを任意に選択することができる。

【００５０】〈具体例２〉具体例２は、ホストコンピュータが顧客の端末２－１，２－２に送信する乱数データに、異なる形状の文字データを混在させるようにしたものである。

【００５１】〈動作〉次に具体例２の動作を説明する。アルファベット文字は、通常、アスキーコード（ASCII：American Standard Code for Information Interchangeコード：米国情報交換用標準符号）で送信されるが、同一のフォントの文字を使用しつづけるとデータの解読は容易になってくる。

【００５２】具体例２では、異なるフォントの文字データを混在させたランダムパターンを送信する。図６は異なるフォントの文字データを示す説明図である。フォントは既存のものでもよいが、人間には認識できてコンピュータでは読みにくいフォントを作成してもよい。そしてできるだけ多く準備しておく。

【００５３】このように異なるフォントの文字データを混在させてランダムパターンを送信すれば、たとえ第三者がトラッププログラムを作成してランダムパターン及

び記憶キーを解読しようとしても、トラッププログラムに精度の高い手書き文字認識プログラムを組み込まない限り、文字データの抽出は困難となり、ランダムパターンの再構成も困難となる。その一方で、異なるフォントの文字データが混在していても、顧客はディスプレイ上で文字データを認識でき、顧客のデータ入力の負担は変わらない。

【００５４】〈効果〉以上、説明したように具体例２によれば、ホストコンピュータから顧客の端末に、異なるフォントが混在したランダムパターンを送信するようにしたので、第三者への情報の漏洩をさらに確実に防止することができる。

【００５５】〈具体例３〉具体例３は、第三者への情報の漏洩をさらに確実に防止するため、端末２－１，２－２側でパスワードに特定の演算を施して送信し、ホストコンピュータ１側で同じ特定の演算を施して送信されたデータ列が顧客のパスワードかどうかを調べるようにしたものである。尚、具体例３と同一要素については同一符号を付して説明を省略する。

【００５６】〈動作〉次に具体例３の動作を説明する。具体例３では、ホストコンピュータ１は顧客の端末２－１，２－２に、記憶キーを用いて得られたパスワードに特定の演算を行うように指示する。

【００５７】顧客はその指示に従って特定の演算を行う。この演算を行うには、顧客の端末２－１，２－２を用いてもよいが、パスワードを盗まれないようにするためには、データの記憶が可能なoneway（一方向性）関数を簡単に計算できる計算機が理想的である。また、その代替として極めて広く普及しているメモリ付きの８桁程度の電卓を用いてもよい。

【００５８】従って、ホストコンピュータ１は、このような電卓でできる程度の演算を指示する。そして、端末２－１，２－２には、演算したパスワードを入力する。

【００５９】図７はホストコンピュータ１の指示内容を示すフローチャートであり、図８はその説明図である。ステップ２１では、パスワードを複数のデータに分けて前半のデータＡを入力する。このように、パスワードを複数のデータに分けるのは、分けたデータ間での演算により、入力情報が漏洩しても元データを推測しにくくするためである。

【００６０】尚、データを入力する前に電卓の表示データを保持するレジスタ、メモリをクリアしておく。

【００６１】ステップ２２では、図８に示すように、この前半のデータＡをメモリにコピーする。ステップ２３では、後半のデータＢを入力する。レジスタの値は、図８に示すようにデータＢとなる。

【００６２】ステップ２４では、データＡとＢとの二項演算を行う。二項演算とは、Ａ＋Ｂのように２つの数から１つの数を作る演算、単項演算とは、$\sqrt{}$Ａのように１つの数から１つの数を作る演算である。この二項演算によって得られたデータをｆ（Ａ，Ｂ）とする。尚、この二項演算は、データＡとＢとから１つの数値が桁あふれなく得られるような演算であれば、どのような演算であってもよい。

【００６３】ステップ２５では、データｆ（Ａ，Ｂ）とデータＡとの二項演算を行う。ステップ２４と同じように、この二項演算も桁あふれが起きなければどのような演算でもよい。この二項演算によって得られたデータをｇ（Ａ，Ｂ）とする。

【００６４】ステップ２６では、ｆ（Ａ，Ｂ）の平方根を算出する。この平方根の演算により、桁あふれがなく、データＡとＢの各桁の数値が混じり合う。即ち、上位の全ての桁について、その数値の変化が下位の桁の数値に伝搬する。言い換えると、例えばｋ桁目の数値は、ｋ桁以上の桁の数値に依存し、ｋ桁よりも上位桁の数値の変化がｋ桁目の数値に現れる。尚、この演算は、平方根演算に限られるものではなく、結果の一部の桁から元の数値の桁の一部が推測できないような単項演算ならばどのような演算であってもよい。

【００６５】ステップ２７では、ｆ（Ａ，Ｂ）の平方根の桁落としを行う。この桁落としによって得られた値をパスワードPassword-fとする。尚、桁落としとは、得られた数値の特定の一部の桁のみを選び、残りを捨てる操作である。そのデータの整数部は多くても４桁、abcd.efghkl...の形になる。ここで、この最初の桁の数値ａが第三者に漏洩すると、このデータがわかってしまうので、例えばcdefghを入力パスワードとするようディスプレイで指示する。ステップ２８では、ステップ２６と同じようにｇ（Ａ，Ｂ）の平方根を算出する。

【００６６】ステップ２９では、ｇ（Ａ，Ｂ）の平方根の桁落としを行う。この桁落としによって得られた値をパスワードPassword-gとする。ステップ３０では、パスワードPassword-fを送信する。ステップ３１では、パスワードPassword-gを送信する。

【００６７】ホストコンピュータ１は、このパスワードPassword-f、Password-gを受信したとき、顧客が用いたのと同じ記憶キーを用いて全てのデータ列に対して図７に示すフローチャートに示す演算を実行し、その中に受信したパスワードPassword-f、Password-gと一致するものがあれば受信したデータ列は顧客のパスワードであると判定して顧客を認証し、不一致であればアクセスを拒絶する。

【００６８】〈効果〉以上、説明したように具体例３によれば、記憶キーを用いて得られたパスワードを２つに分けて特定演算の中に平方根を求める演算を含めて桁の数値が混在するようにしたので、第三者への情報の漏洩をさらに確実に防止することができ、記憶キーが盗まれる危険性が小さくなる。

【００６９】〈具体例４〉具体例４は、ホストコンピュータ１側で復元したパスワードのうち、桁落としされた

11

データを顧客の端末2－1，2－2に送信し、顧客の端末2－1，2－2の側でも管理者を認証できるようにしたものである。

【0070】例えば、顧客が商店Sに所定の商品を注文し、クレジット会社が商店Sに商品の支払をする場合を考える。この場合、図1において、端末2－1，2－2をそれぞれ顧客の端末、商店の端末とし、ホストコンピュータ1はクレジット会社のコンピュータであるものとする。尚、具体例1と同一要素については同一符号を付して説明を省略する。

【0071】〈動作〉この場合、顧客を管理するホストコンピュータを1つにして管理者であるクレジット会社が顧客の認証を行う。インターネット上の商店等がこのクレジット会社に顧客の認証を依頼する。このようなシステムにすれば有利であり、安全である。

【0072】顧客は端末2－1から商店Sの端末2－2に商品の注文をする。顧客から注文を受けた商店Sは、自己の端末2－2をクレジット会社のホストコンピュータ1に接続し、パスワードを入力して自己の商店の認証を受け、それから顧客の認証を依頼する。

【0073】クレジット会社と商店との間では、顧客とは異なり、移動性、汎用性が要求されないため、通常のoneway関数による認定を行う。次に顧客も自己の端末2－1をクレジット会社のホストコンピュータ1に接続する。クレジット会社はホストコンピュータ1を用いて具体例1と同じように顧客の認証を行う。

【0074】例えば、顧客の端末2－1がインターネットカフェ（インターネットに接続しているコンピュータが置いてある喫茶店）の端末である場合には、クレジット会社の認証がシミュレートされて情報が盗まれる危険＊性は大きい。

12

【0075】従って、顧客から桁落としが行われて送信されたパスワードのうち、クレジット会社は、桁落としによって入力されなかった桁の数値を顧客に送信する。この数値が、顧客が計算した数値と一致したときは、顧客が管理者を認証する。また、不一致のとき、顧客はそのシステムの管理者にただちに通報する。

【0076】〈効果〉以上、説明したように具体例4によれば、桁落としをした数値の一部を顧客に返送することにより、顧客も管理者の認証を行うことができる。

【図面の簡単な説明】

【図1】具体例1の構成を示すブロック図である。

【図2】ホストコンピュータ、端末の構成を示すブロック図である。

【図3】具体例1の動作を示すフローチャートである。

【図4】具体例1のディスプレイに表示されたランダムパターンを示す説明図である。

【図5】具体例1の記憶キーの一例を示す説明図である。

【図6】具体例2の動作を示す説明図である。

【図7】具体例3のホストコンピュータの指示内容を示すフローチャートである。

【図8】具体例3の動作を示す説明図である。

【図9】従来のワンタイムパスワードの動作を示す説明図である。

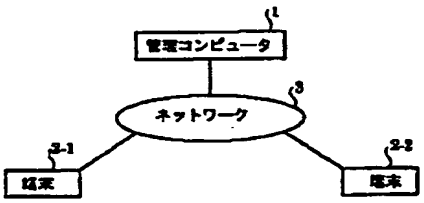
【符号の説明】

1　ホストコンピュータ

2－1，2－2　端末

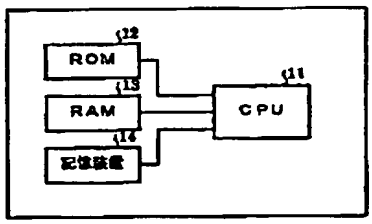
3　ネットワーク

【図1】



具体例1のシステム構成図

【図2】



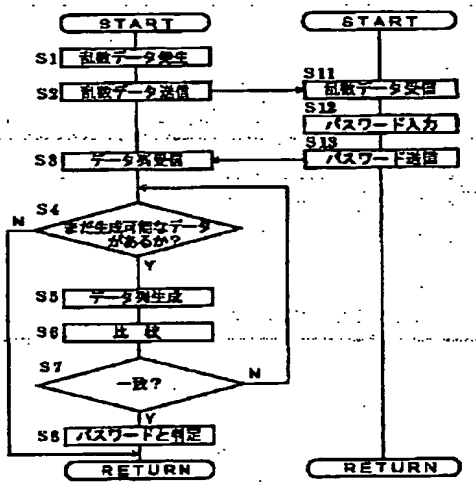
具体例1のホストコンピュータ端末の構成を示すブロック図

【図6】

1 1 1 2 2 3 3 ... 0 0

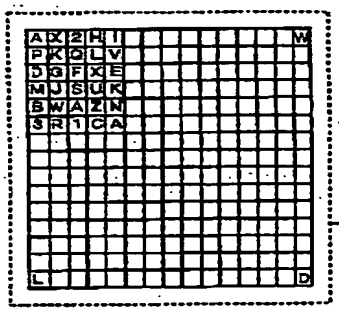
具体例2の動作を示す説明図

【図3】



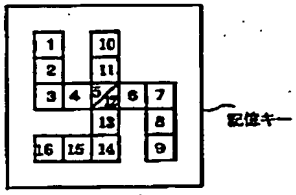
具体例1の動作を示すフローチャート

【図4】



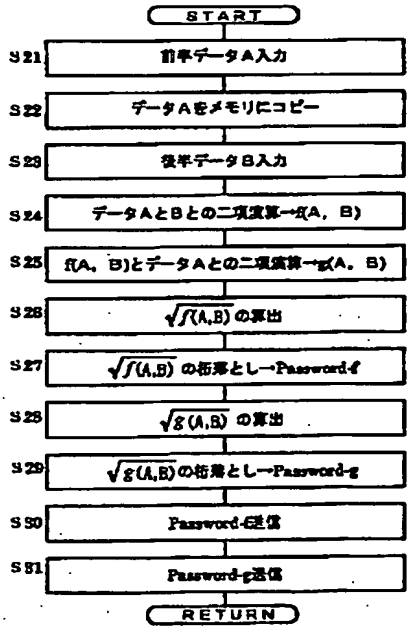
具体例1のディスプレイ上に表示されたランダムパターンを示す説明図

【図5】



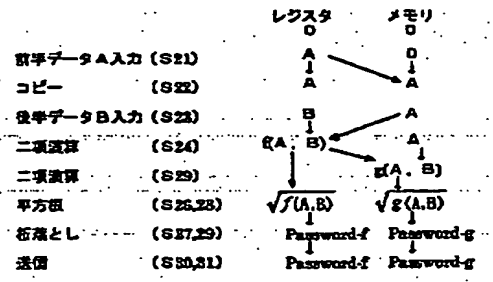
具体例1の記憶キーの一例

【図7】



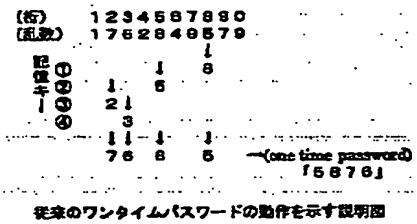
具体例3のホストコンピュータの指示内容を示すフローチャート

【図8】



具体例3の動作を示す説明図

【図9】



従来のワンタイムパスワードの動作を示す説明図